Rolls-Royce

SPINLINE 3 Digital Safety I&C Platform

- Software Components
- Software Tools
- Software Development Process

January 07, 2010
Non-proprietary

Topics

- ***SPINLINE 3*** Safety Software Components:
  - Generic Platform Software
  - Plant-specific Application Software
- Sofware Tools:
  - SCADE
  - CLARISSE
- Application Software Development Process

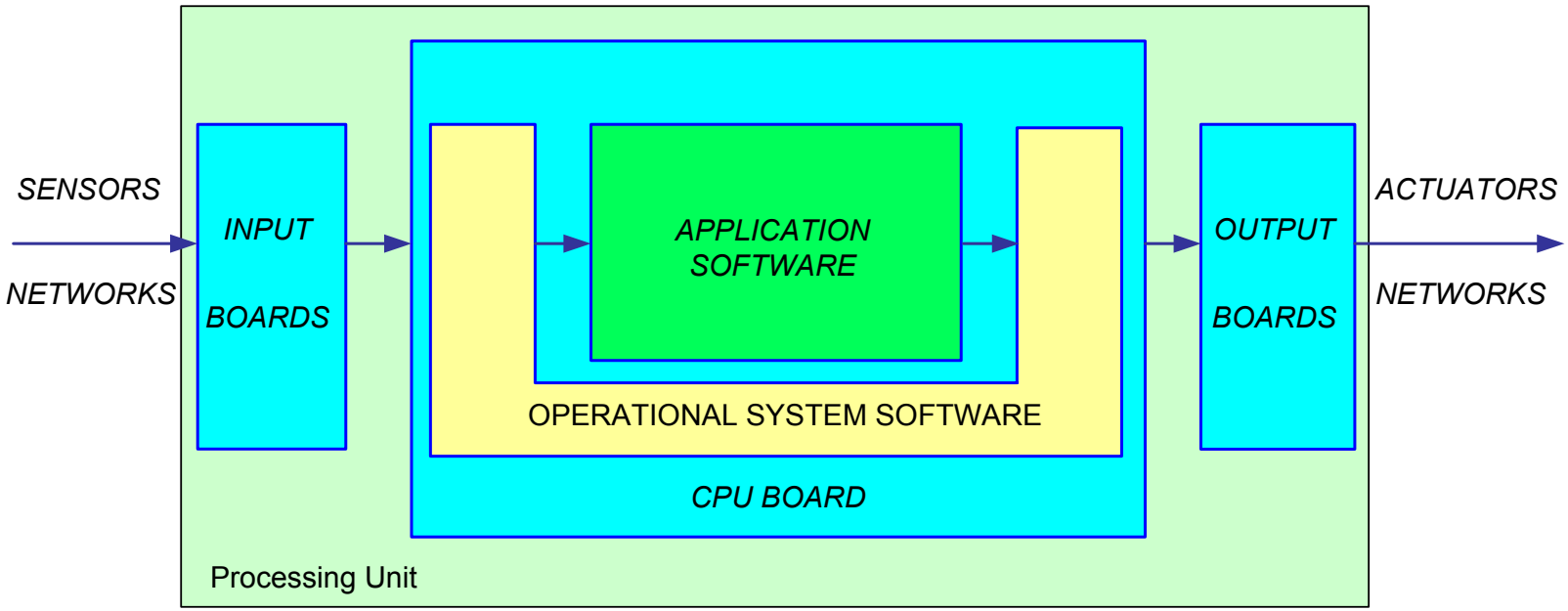
Rolls-Royce

SPINLINE 3 Safety *Software Components*

Safety Software Components

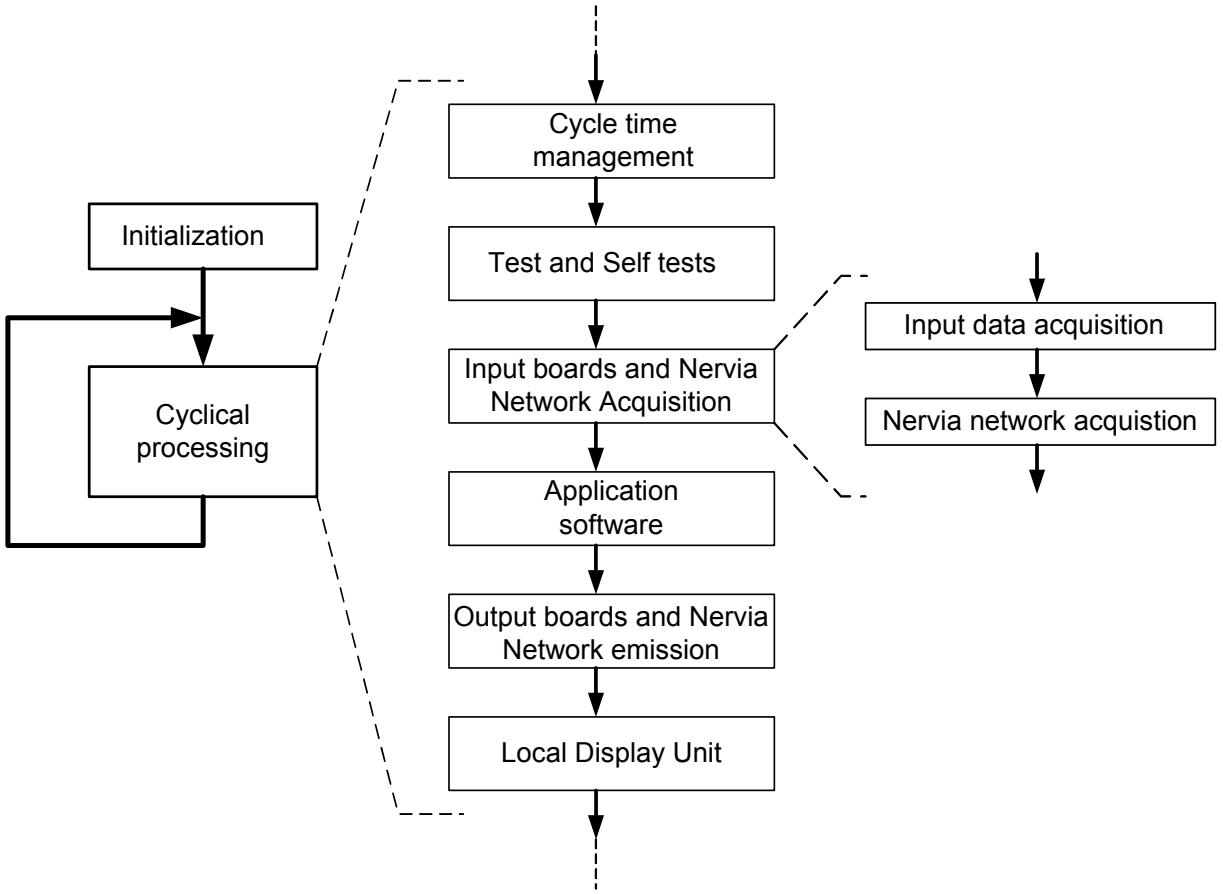
- Generic Platform Software, which is comprised of the following standard items:
  - Operational System Software (OSS)
    - Low complexity: single loop, no interrupts, dedicated to safety I&C needs
    - Category A qualified: designed and V&V according to IEC 60880
    - Application independent
    - Developed and maintained by RRCN
    - Fully available under confidentiality agreement for licensing purposes
  - Application-oriented library
  - Software Embedded in I/O boards
- Plant-specific application software
  - Dedicated to the customers' needs
  - Developed using the CLARISSE System and Software Development Environment (SSDE) and the SCADE language

Safety Software Components Installed on a Processing Unit



Processing Unit Software Architecture

- The ***SPINLINE 3*** safety software installed on each processing unit (i.e., the OSS and application software) performs sequentially, deterministically and periodically a set of functions



Operational System Software (OSS)

- "Operational System Software" versus "Operating System"
  - Defined in IEC 60880 Ed2 as: "Software running on the target processor during operation, such as input/output drivers and services, interrupt management, scheduler, communication drivers, application-oriented libraries, on-line diagnostic, redundancy and graceful degradation management"
  - It differs from an Operating System (OS) which provides far more complex sets of services for general purpose computers (i.e., support for file management, multi-users access, dynamic memory management, multi-threaded processes).

- The ***SPINLINE 3*** system software is a minimum and simple Operational System Software
  - It provides only the services needed for nuclear safety applications:
    - I/O and communication control
    - Interface between the software application and the equipment
    - hardware self-tests
    - Monitoring of cyclical execution of application software
  - It does not include functions recognized to be of unnecessary complexity for implementation of nuclear safety I&C functions.

Application-Oriented Library

- This library is a collection of re-usable software components that can be used by developers when designing application software using the SCADE tool. These re-usable components include:
  - Logic functions
  - Numeric functions
- The library components were developed and are maintained according to the same basic software life cycle processes and Quality Assurance Program applicable to the OSS.

Software Embedded in I/O boards

- Embedded software is employed in the following ***SPINLINE 3*** electronic boards:
  - Calibrated pulse acquisition board (ICTO board) where the processing is implemented using an Intel 8031 microprocessor
  - NERVIA+ communication board, installed on the CPU board, where the processing is implemented using a Motorola MPC860 communication controller

- The Class 1E software embedded in I/O and communication boards was developed according to the RRCN life cycle process and Quality Assurance Program applicable to Class 1E software that was used for the development of the OSS

PLD embedded in electronic boards

- Programmable Logic Device (PLD) is employed in the following ***SPINLINE 3*** electronic boards:
  - Antifuse FPGA used to implement hardware logic functions on the CPU25+ Board
  - Antifuse FPGA used to implement hardware logic function and acquisition processing on the analog 16EANA ISO input board
  - CPLD used to implement hardware logic functions on the NERVIA+ daughter board
- These components perform functions that contribute to the performance of the safety functions. However, the logic in each of these component is standardized, and does not depends on the safety function being implemented in the ***SPINLINE 3*** system.
- the function of the PLD is developed according to a specific development process which is part of the RRCN Electronic hardware design process and is not documented in this LTR

Plant-specific Application Software

- Implements the application functions:
  - "Application function" is defined in IEC 60880 Ed2 as: "Function of an I&C system that performs a task related to the process being controlled rather than to the functioning of the system itself"
  - "Application functions" are specified in the requirements, using either:
    - textual description
    - functional diagrams, or
    - implementation diagrams (for refurbishment)
- RRCN describes the application using the SCADE tool.
- The application is translated into executable code by CLARISSE production tools.

Characteristics of ***SPINLINE 3*** Safety Software

- Operating safety
  - Defensive programming
  - Write-protected software
  - Physical access to the CPU board is necessary for software modifications
- "Transparency“
  - All safety software components are reviewable
  - No Safety software «black boxes»

Tool Description: SCADE - Safety Critical Application Development Environment

SCADE Overview

- A language and a set of tools dedicated to the development of Safety Critical Applications
- Provides block diagram formalism with rigorous textual & graphical syntax and well defined semantic
- User-friendly: it does not require specialized programming skills

SCADE Main Features

- Synchronous and data-flow approaches
- Graphical function block diagram (FBD) formalism with formal semantic
- Support top-down design methodology
- Automated syntactic & semantic verifications (deadlocks, types, completeness, consistency, variables initialization ...)
- Support for reuse of components

SCADE History (1/2)

- Before 1984
  - design & code were performed manually
- 1984
  - first definition of a graphical dataflow language
- 1985
  - formal semantic added by the Grenoble software engineering laboratory - (LGI) : subset of the LUSTRE synchronous language
- 1986
  - development of the SAGA tool diagram editor, code generator used for experimental reactors and N4 plants
  - highly positive feedback of experience
- 1991
  - contract with VERILOG to develop a Unix version of SAGA (Xwindows / motif editor, new code generator)

SCADE History (2/2)

- 1993
  - AEROSPATIALE (Airbus consortium) chooses LUSTRE to enhance his proprietary graphical specification
  - AEROSPATIALE / SCHNEIDER ELECTRIC/ VERILOG agreement
- 1996
  - SCADE available on the market from VERILOG company
  - First use by Schneider Electric for the KOSLODUY contract
- 1998
  - European ESPRIT project : CRISYS
  - EDF: CP0 contract with FRAMATOME / SCHNEIDER ELECTRIC
- Now
  - SCADE is used for TIHANGE, QINSHAN, FESSENHEIM, BUGEY, DUKOVANY, IGNALINA
  - A version of SCADE is used by Airbus Industries to develop the critical embedded software for A340 and A380 airplanes
  - SCADE is now supported and distributed by ESTEREL Technologies

SCADE Example

SCADE Example: Functional Diagram

SCADE Operators Used in the Example (1/2)

SCADE Operators Used in the Example (2/2)

SCADE Diagram: Main View

SCADE Diagram: Parameters

SCADE Diagram: Network Output

SCADE Diagram: Linear Conversion

SCADE Diagram: Threshold Comparison

More on the *THRESHOLD_COMP* Component

SCADE Graphic Editor View

Rolls-Royce

Tool Description: CLARISSE

CLARISSE Overview

- Objectives
  - Production of high quality software applications for safety systems
  - Guaranty of data consistency
  - Increase of development productivity
- Intended primarily for the development of ***SPINLINE 3*** safety I&C systems for nuclear plants
- CLARISSE is a component of the ***SPINLINE 3*** System Engineering Tool

CLARISSE Within the System Engineering Tools (SPEED)

CLARISSE - Main Features

Plant-specific System & Software Development

CLARISSE - System Level Descriptions

CLARISSE - Processing Units Descriptions

CLARISSE - Software Production

Software Development Process for a Plant-Specific Application

Application Software Project Plans Preparation

Application Software Life Cycle Development Activities

Comments on the application software life cycle development chart

Software Development Life Cycle with CLARISSE